Finite Fields and Their Applications **5,** 364–377 (1999)
Article ID ffta.1999.0255, available online at http://www.idealibrary.com on IDEAL®

# Curves with Many Points and Multiplication Complexity in Any Extension of $\mathbb{F}_q$

Stéphane Ballet

*C.N.R.S. Institut de Mathématiques de Luminy, Luminy Case 907, F13288 Marseille Cedex 9, France*
E-mail: ballet@iml.univ-mrs.fr

*Communicated by Michael Tsfasman*

Received July 8, 1998; revised March 2, 1999

From the existence of algebraic function fields having some good properties, we obtain some new upper bounds on the bilinear complexity of multiplication in all extensions of the finite field $\mathbb{F}_q$, where $q$ is an arbitrary prime power. So we prove that the bilinear complexity of multiplication in the finite fields $\mathbb{F}_{q^n}$ is linear uniformly in $q$ with respect to the degree $n$. © 1999 Academic Press

*Key Words*: Bilinear complexity; finite fields; algebraic function fields; algebraic curves.

## 1. INTRODUCTION—NOTATIONS

### 1.1. *Bilinear Complexity of Multiplication*

Let $\mathbb{F}_q$ be a finite field with $q$ elements where $q$ is a prime power and let $\mathbb{F}_{q^n}$ be an $\mathbb{F}_q$ extension of degree $n$. Let $P(X) \in \mathbb{F}_q[X]$ be a monic irreducible over $\mathbb{F}_q$ of degree $n$. Then $\mathbb{F}_{q^n}$ is constructed as the field $\mathbb{F}_q[X]/(P(X))$ and so any element of $\mathbb{F}_{q^n}$ is represented by a polynomial of degree $\leq n-1$ with coefficients in $\mathbb{F}_q$. Consequently the multiplication of two elements of $\mathbb{F}_{q^n}$ corresponds to the multiplication in $\mathbb{F}_q[X]$ modulo $P(X)$. For any integer $n$, let us consider the multiplication $m$ in the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$ of dimension $n$. The multiplication $m$ is a bilinear map from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ into $\mathbb{F}_{q^n}$, thus it corresponds to a linear map from the tensor product $\mathbb{F}_{q^n} \otimes \mathbb{F}_{q^n}$ over $\mathbb{F}_q$ into $\mathbb{F}_{q^n}$:

$$M : \mathbb{F}_{q^n} \otimes \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}.$$

More precisely, $m = M \circ \phi$, where $\phi$ is the canonical embedding from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ in the tensor product $\mathbb{F}_{q^n} \otimes \mathbb{F}_{q^n}$ defined by $\phi(x, y) = x \otimes y$. One can also



1071-5797/99 $30.00

represent $M \in \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^n} \otimes \mathbb{F}_{q^n}, \mathbb{F}_{q^n})$ by a tensor $t_M \in \mathbb{F}_{q^n}^* \otimes \mathbb{F}_{q^n}^* \otimes \mathbb{F}_{q^n}$, where $\mathbb{F}_{q^n}^* = \mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_{q^n}, \mathbb{F}_q)$ denotes the dual of $\mathbb{F}_{q^n}$. Hence the product of $x$ and $y$ is the convolution of this tensor with $x \otimes y \in \mathbb{F}_{q^n} \otimes \mathbb{F}_{q^n}$. If

$$t_M = \sum_{l=1}^{\lambda} a_l \otimes b_l \otimes c_l, \tag{1}$$

where $a_l \in \mathbb{F}_{q^n}^*$, $b_l \in \mathbb{F}_{q^n}^*$, $c_l \in \mathbb{F}_{q^n}$, then

$$x \,.\, y = \sum_{l=1}^{\lambda} a_l(x) b_l(y) c_l. \tag{2}$$

Every expression (2) is called a bilinear multiplication algorithm $\mathscr{U}$. The number $\lambda$ is called the multiplicative complexity $\mu(\mathscr{U})$ *of* $\mathscr{U}$.

Let us set

$$\mu_q(n) = \min_{\mathscr{U}} \mu(\mathscr{U}),$$

where $\mathscr{U}$ is running over all bilinear multiplication algorithms in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Then $\mu_q(n)$ is called the bilinear complexity of multiplication in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and it corresponds to the minimum possible number of summands in any tensor decomposition of type (1).

Let us give the definition of the following asymptotic parameter:

$$\mathscr{M}_q = \limsup_{n \to \infty} \mu_q(n)/n.$$

### 1.2. *Basic Facts on the Algebraic Function Fields of One Variable*

Let $F/\mathbb{F}_q$ be an algebraic function field of one variable of genus $g$, over the constant field $\mathbb{F}_q$, associated to a smooth, absolutely irreducible curve $X$ over $\mathbb{F}_q$. Let $\mathrm{Div}(F/\mathbb{F}_q)$ be the divisor group of the algebraic function field $F$ over $\mathbb{F}_q$, i.e., the free abelian group generated by the places of the algebraic function field $F$ over $\mathbb{F}_q$. Let $P_1(F/\mathbb{F}_q)$ be the set of degree one places of $F$ over $\mathbb{F}_q$ and $N(F/\mathbb{F}_q)$ be the cardinality of $P_1(K/\mathbb{F}_q)$. The number $N(F/\mathbb{F}_q)$ satisfies the Hasse–Weil inequality $N(F/\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$. In particular, an algebraic function field defined over $\mathbb{F}_{q^2}$ is called maximal if $N(F/\mathbb{F}_{q^2})$ reaches the Hasse–Weil bound. Setting $N_q(g) = \{N(F/\mathbb{F}_q) | F/\mathbb{F}_q$ is a function field of $\mathbb{F}_q$ of genus $g\}$ and $A(q) = \limsup_{g \to \infty} N_q(g)/g$, we know that $A(q)$ satisfies the Drinfeld–Vladut bound $A(q) \leq \sqrt{q} - 1$ [12]. Let us denote by $\mathscr{P}_F$ the set of principal divisors and by $\mathrm{Div}^0(F/\mathbb{F}_q)$ the set of degree zero divisors which are both subgroups of $\mathrm{Div}(F/\mathbb{F}_q)$. We denote by $[\mathscr{D}]$ the class of a divisor $\mathscr{D}$ modulo $\mathscr{P}_F$. Let $\mathrm{Pic}(X)$ be the Picard group that is the group of the

arbitrary degree divisor classes modulo $\mathscr{P}_F$. Let $\mathrm{Pic}^0(X)$ be the finite group of the degree zero divisor classes modulo $\mathscr{P}_F$. Let $h(F/\mathbb{F}_q)$ be the order of $\mathrm{Pic}^0(X)$, called the class number of $F/\mathbb{F}_q$. If $\mathscr{D}$ is a divisor then $\mathscr{L}(\mathscr{D}) = \{f \in F, \mathscr{D} + (f) \geq 0\} \cup \{0\}$ defines a vector space over $\mathbb{F}_q$ whose dimension $l(\mathscr{D})$ is given by the Riemann–Roch theorem. We denote by $\mathscr{K}$ a canonical divisor. A divisor $\mathscr{D}$ is called non-special if $l(\mathscr{K} - \mathscr{D}) = 0$; otherwise $\mathscr{D}$ is called special. A divisor of the form $\mathscr{D} = P$ where $P$ is a place of $F/\mathbb{F}_q$, is called a prime divisor. For any place $P$ we define $F_P$ to be the residue class field of $P$ which is a finite extension of $\mathbb{F}_q$. The degree of a divisor $\mathscr{D} = \sum_P a_P P$ is defined by $\deg \mathscr{D} = \sum_P a_P \deg P$, where $\deg P$ is the dimension of $F_P$ over $\mathbb{F}_q$. The order of a divisor $\mathscr{D} = \sum_P a_P P$ in $P$ is the number $a_P$ denoted $\mathrm{ord}_P \mathscr{D}$. The support of a divisor $\mathscr{D}$ is the set supp $\mathscr{D}$ of the places $P$ such that $\mathrm{ord}_P \mathscr{D} \neq 0$. The divisor $\mathscr{D}$ is called effective if $\mathrm{ord}_P \mathscr{D} \geq 0$ for any $P$.

### 1.3. *Known Results*

The bilinear complexity $\mu_q(n)$ of multiplication in the $n$ degree extension of a finite field $\mathbb{F}_q$ with $q$ elements is known for certain values of $n$. In particular, Winograd [14] and de Groote [8] have shown that this complexity is $\geq 2n - 1$, with equality holding if and only if $n \leq \frac{1}{2}q + 1$. Moreover, Lempel *et al.* [9] have proved that the bilinear complexity of multiplication in any finite field $\mathbb{F}_{q^n}$ is such that $\mu_q(n) \leq f_q(n)n$, where $f_q(n)$ is asymptotically a very slowly growing function. On the other hand, using interpolation on algebraic curves, Chudnovsky and Chudnovsky in [3] have succeeded in obtaining a principle of construction of fast multiplication algorithms. Shparlinski *et al.* [11] have studied this principle and found new asymptotic bounds. More precisely, they have proved that for any prime power $q \geq 3$, $\mathscr{M}_{q^2} \leq 2(1 + \frac{1}{q-2})$, $\mathscr{M}_q \leq 6(1 + \frac{1}{q-2})$, and $\mathscr{M}_2 \leq 27$, where $\mathscr{M}_q = \limsup_{n \to \infty} \mu_q(n)/n$. Using the principle of the D. V. and G. V. Chudnovsky algorithm applied to elliptic curves, M. A. Shokrollahi has shown in [10] that the bilinear complexity of multiplication is equal to $2n$ for $\frac{1}{2}q + 1 < n < \frac{1}{2}(q + 1 + 2\varepsilon(q))$, where $\varepsilon$ is the function defined by:

$$\varepsilon(q) = \begin{cases} \text{greatest integer} \leq 2\sqrt{q} \text{ prime to } q & \text{if } q \text{ is not a perfect square} \\ 2\sqrt{q} & \text{if } q \text{ is a perfect square.} \end{cases}$$

Recently, in [1], we have generalized to algebraic function fields the study made by Shokrollahi. We have proved that if there exists an algebraic function field $F/\mathbb{F}_q$ of genus $g$ containing a prime divisor $Q$ of degree $n$, a non-special divisor of degree $g - 1$ and more than $2n + 2g - 2$ places of degree one, then $\mu_q(n) \leq 2n + g - 1$ (cf. Theorem 2.1 [1]). In particular, we have shown that the maximal algebraic function fields $F/\mathbb{F}_{q^2}$ satisfy these properties and have deduced from them some new bounds on the

multiplication complexity $\mu_{q^2}(n)$ for certain values of $n$, which are recalled in Section 4.

### 1.4. *New Results Established in This Paper*

Now, our main purpose is to find some new bounds on the multiplication complexity in some extensions of an arbitrary field $\mathbb{F}_q$. In this paper, we mainly prove that the bilinear complexity of multiplication in any finite field $\mathbb{F}_{q^n}$ where $q$ is an arbitrary prime power, is such that $\mu_q(n) \leq B_q n$ where $B_q$ is defined by

$$B_q = \begin{cases} 6\left(1 + \frac{q}{q-3}\right) & \text{if } q > 3 \\ 2\left(1 + \frac{\sqrt{q}}{\sqrt{q}-3}\right) & \text{if } q > 9 \text{ and } q \text{ is a perfect square} \\ 45 & \text{if } q = 3 \\ 90 & \text{if } q = 2. \end{cases}$$

So we prove that the bilinear complexity of multiplication in the finite fields $\mathbb{F}_{q^n}$, where $q$ is an arbitrary prime power, is linear uniformly in $q$ with respect to the degree $n$. To this end, we first establish the following general theorem in Section 2, which is stronger than Theorem 2.1 in [1]:

THEOREM 1.1. *Let $q$ be a prime power and let $n > 1$ be a natural number. If there exists an algebraic function field $F/\mathbb{F}_q$ of genus $g$ satisfying the conditions*

(1) *$F/\mathbb{F}_q$ contains a prime divisor $Q$ of degree $n$,*

(2) *$N(F/\mathbb{F}_q) > 2n + 2g - 2$,*

*then*

$$\mu_q(n) \leq 2n + g - 1.$$

The aim of this paper is to prove this theorem and the existence of algebraic function fields having these properties in order to give new bounds for the large extensions of $\mathbb{F}_q$. If $q$ is totally arbitrary, the problem is difficult. Thus, in Section 3 we limit our study to algebraic function fields defined over $\mathbb{F}_{q^2}$. In that section, we use the tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound described by A. Garcia and H. Stichtenoth in [7]. From it, we show that for any prime power $q \geq 3$ and for all natural numbers $n > \frac{1}{2}q^2 + 1$, there exist algebraic function fields over $\mathbb{F}_{q^2}$ satisfying the conditions of Theorem 1.1. Finally, in Section 4, from the results obtained in Section 3, we give new bounds on the multiplication complexity in any extension of $\mathbb{F}_q$ for any prime power $q$.

## 2. INTERPOLATION IN ALGEBRAIC FUNCTION FIELDS

In this section, we establish Theorem 1.1 which ensures the existence of an algorithm of complexity $\leq 2n + g - 1$ whenever there exists an algebraic function field of genus $g$ over $\mathbb{F}_q$ having some good properties.

We will prove this theorem after establishing the following Lemmas 1 and 2.

LEMMA 2.1. *Let $q$ be a prime power. Let $F/\mathbb{F}_q$ be an algebraic function field of genus $g$ containing at least $g+1$ places of degree one. Suppose that $T \subseteq P_1(F/\mathbb{F}_q)$ is a set of places of degree one such that $|T| \geq g+1$. Then there exists a non-special divisor $\mathscr{R}$ with $\deg \mathscr{R} = g-1$ and $\operatorname{supp} \mathscr{R} \subseteq T$.*

*Proof.* Under these assumptions, we know that there exists a non-special divisor $\mathscr{B} \geq 0$ with $\deg \mathscr{B} = g$ and $\operatorname{supp} \mathscr{B} \subseteq T$ by Proposition I.6.10 in [12]. Hence, by the Riemann–Roch theorem, $l(\mathscr{B}) = 1$ because $\mathscr{B}$ is non-special. Let $\mathscr{P} \in T$ be a place of degree one such that $\mathscr{P}$ does not belong to $\operatorname{supp} \mathscr{B}$. Let us consider the divisor $\mathscr{R} = \mathscr{B} - \mathscr{P}$. First, note that we have clearly $\operatorname{supp} \mathscr{R} \subseteq T$. Then $\mathscr{L}(\mathscr{R}) = \mathscr{L}(\mathscr{B} - \mathscr{P}) \subseteq \mathscr{L}(\mathscr{B})$ and as $\mathscr{B}$ is effective, $\mathbb{F}_q \subseteq \mathscr{L}(\mathscr{B})$. Moreover, it is clear that $\mathbb{F}_q \cap \mathscr{L}(\mathscr{B} - \mathscr{P}) = \{0\}$, thus $l(\mathscr{R}) = 0$. As moreover $\deg \mathscr{R} = g - 1$, it follows that $\mathscr{R}$ is non-special, which gives the result. ■

Let Lemma 2.2 be under the assumptions of Theorem 1.1.

LEMMA 2.2. *There exists a divisor $\mathscr{D}$ such that*:

(1) *The evaluation map $E$ defined by*

$$\begin{aligned} E : \mathscr{L}(\mathscr{D}) &\to F_Q \\ f &\mapsto f(Q) \end{aligned}$$

*is an isomorphism of vector spaces over $\mathbb{F}_q$.*

(2) *There exist the places of degree one $P_1, \ldots, P_{\dim \mathscr{L}(2\mathscr{D})}$ such that the evaluation map $T$ defined by*

$$\begin{aligned} T : \mathscr{L}(2\mathscr{D}) &\to \mathbb{F}_q^{\dim \mathscr{L}(2\mathscr{D})} \\ f &\mapsto (f(P_1), \ldots, f(P_{\dim \mathscr{L}(2\mathscr{D})})) \end{aligned}$$

*is an isomorphism.*

*Proof.* The divisor $Q$ is of degree $n$, hence the residue class field $F_Q$ of $Q$ is isomorphic to $\mathbb{F}_{q^n}$. Since $N > 2n + 2g - 2 \geq g + 1$ for all $n > 1$, there exists a non-special divisor $\mathscr{R}$ with $\deg \mathscr{R} = g - 1$ by Lemma 2.1. Then we choose a divisor $\mathscr{D}_1$ such that $\mathscr{D}_1 = \mathscr{R} + Q$. Let $[\mathscr{D}_1]$ be the class of $\mathscr{D}_1$, then by [4],

Lecture 14, Lemma 1, [$\mathscr{D}_1$] contains a divisor $\mathscr{D}$ defined over $\mathbb{F}_q$ such that $\operatorname{ord}_P \mathscr{D} = 0$ for all prime divisors of degree one and $\operatorname{ord}_Q \mathscr{D} = 0$. Since $\operatorname{ord}_Q \mathscr{D} = 0$, $\mathscr{L}(\mathscr{D})$ is contained in the valuation ring $O_Q$ of $Q$. Hence $E$ is a restriction of the residue class mapping, and defines an $\mathbb{F}_q$-algebra homomorphism. The kernel of $E$ is $\mathscr{L}(\mathscr{D} - Q)$. But $\mathscr{D} - Q$ is non-special of degree $g - 1$, then $l(\mathscr{D} - Q) = \deg(\mathscr{D} - Q) - g + 1 = 0$ and $E$ is injective. Moreover, of $\mathscr{K}$ is a canonical divisor, we have $l(\mathscr{D}) = l(\mathscr{K} - \mathscr{D}) + n$ by the Riemann–Roch theorem. Hence, $l(\mathscr{D}) \geq n$ and as $E$ is injective, we obtain $l(\mathscr{D}) = n$. We conclude that $E$ is an isomorphism. Let $\mathscr{P} = \{P_1, \ldots, P_N\}$ be the set of prime divisors of degree one of $F/\mathbb{F}_q$. Let the evaluation map $T_{\mathscr{P}}$ be defined by

$$\begin{aligned} T_{\mathscr{P}}: \mathscr{L}(2\mathscr{D}) &\to \mathbb{F}_q^N \\ f &\mapsto (f(P_1), \ldots, f(P_N)). \end{aligned}$$

This map $T$ is well defined because $\mathscr{L}(2\mathscr{D})$ is contained in the valuation ring of every prime divisor of degree one. Moreover, the kernel of $T_{\mathscr{P}}$ is $\mathscr{L}(2\mathscr{D} - (P_1 + \cdots + P_N))$ which is trivial because $N > 2n + 2g - 2$. Therefore $T_{\mathscr{P}}$ is injective with rank $\dim \mathscr{L}(2\mathscr{D})$. The lemma follows. ■

Now we can prove Theorem 1.1.

*Proof.* Let $S$ be the evaluation function defined by

$$\begin{aligned} S: \mathscr{L}(\mathscr{D}) &\to \mathbb{F}_q^{\dim \mathscr{L}(2\mathscr{D})} \\ h &\mapsto (h(P_1), \ldots, h(P_{\dim \mathscr{L}(2\mathscr{D})})). \end{aligned}$$

This map is well defined for the similar arguments as $T$. Let us denote by $e_1, \ldots, e_{\dim \mathscr{L}(2\mathscr{D})}$ the natural basis of $\mathbb{F}_q^{\dim \mathscr{L}(2\mathscr{D})}$ (i.e., $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$) and by $\Pi_1, \ldots, \Pi_{\dim \mathscr{L}(2\mathscr{D})}$ the dual basis of $e_1, \ldots, e_{\dim \mathscr{L}(2\mathscr{D})}$. Consider the tensor

$$t_M = \sum_{i=1}^{\dim \mathscr{L}(2\mathscr{D})} A_i \otimes A_i \otimes C_i,$$

where $A_i = \Pi_i \circ S \circ E^{-1} \in \mathbb{F}_{q^n}^*$, the dual of $\mathbb{F}_{q^n}$, and $C_i = T^{-1}(e_i)(Q) \in \mathbb{F}_{q^n}$. Note that $A_i$ and $C_i$ are well defined because $E$ and $T$ are isomorphisms by Lemmas 2.1 and 2.2. Now we have to show that $t_M(x \otimes y) = x.y$. Let $f$ and

$g$ be defined by $f = E^{-1}(x)$ and $g = E^{-1}(y)$. Then

$$t_M(x \otimes y) = \sum_{i=1}^{\dim \mathscr{L}(2\mathscr{D})} A_i(x) A_i(y) C_i,$$

$$t_M(x \otimes y) = \sum_{i=1}^{\dim \mathscr{L}(2\mathscr{D})} (\Pi_i \circ S \circ E^{-1}(x)).(\Pi_i \circ S \circ E^{-1}(y))(T^{-1}(e_i)(Q)),$$

thus

$$t_M(x \otimes y) = \sum_{i=1}^{\dim \mathscr{L}(2\mathscr{D})} f(P_i) g(P_i)(T^{-1}(e_i)(Q)),$$

and

$$t_M(x \otimes y) = T^{-1}\left( \sum_{i=1}^{\dim \mathscr{L}(2\mathscr{D})} f(P_i) g(P_i) e_i \right)(Q),$$

therefore

$$t_M(x \otimes y) = (fg)(Q) = f(Q) g(Q) = x.y,$$

and as $\dim \mathscr{L}(2\mathscr{D}) = 2n + g - 1$ by the Riemann–Roch theorem, the proof is complete. ■

*Remark.* In fact, one could get a proof of Theorem 1.1 applying Lemma 14.10 in [2] in conjunction with Lemma 2.2 but we prefer to give an independant proof to be self-contained.

So, we have reduced the assumptions of Theorem 2.1 in [1] without losing information. On the other hand, we can again reduce them but with the restriction that $n$ is large with respect to $g$ or $g$ is small.

COROLLARY 2.1. *Let $q$ be a prime power and $n > 1$ be a natural number. If there exists an algebraic function field $F/\mathbb{F}_q$ of genus $g$ with $2g + 1 \leq g^{(n-1)/2}(q^{1/2} - 1)$ (in particular if $g \leq (n-3)/4$) such that $N(F/\mathbb{F}_q) > 2n + 2g - 2$, then*

$$\mu_q(n) \leq 2n + g - 1.$$

*Proof.* The existence of a prime divisor $Q$ of degree $n$ is given by the inegality $2g + 1 \leq q^{(n-1)/2}(q^{1/2} - 1)$ (in particular if $g \leq (n-3)/4$) by [12, Corollary v.2.10.c p.179]. Finally, the result follows from Theorem 1.1. ■

Now, it is interesting to know if for any $q$ and for any integer $n > \frac{1}{2}q + 1$, there exists an algebraic function field over $\mathbb{F}_q$ satisfying the conditions of Theorem 1.1.

## 3. EXISTENCE OF ALGEBRAIC FUNCTION FIELDS HAVING REQUIRED PROPERTIES

In this section, we consider the tower $F_1 \subseteq F_2 \subseteq F_3 \subseteq \ldots$ of function fields $F_i/\mathbb{F}_{q^2}$ over $\mathbb{F}_{q^2}$ such the ratio $N_i/g_i$ tends to the Drinfeld–Vladut bound $A(q^2) = q - 1$, constructed by Garcia and Stichtenoth in [7]. From it, we show that for any $q \geq 3$ and for almost all $n \in \mathbb{N}$, there exists an algebraic function field having more than $2n + 2g - 2$ places of degree one. First, let us recall the two following results established by Garcia and Stichtenoth in [7].

THEOREM 3.1. *The genus $g_k = g(F_k)$ is given by the following formula*:

$$g_k = \begin{cases} q^k + q^{k-1} - q^{(k+1)/2} - 2q^{(k-1)/2} + 1, & \text{if } k \equiv 1 \mod 2 \\ q^k + q^{k-1} - \frac{1}{2}q^{(k/2)+1} - \frac{3}{2}q^{(k/2)} - q^{(k/2)-1} + 1, & \text{if } k \equiv 0 \mod 2. \end{cases}$$

*Let $N_k$ be the number of places of $F_k/\mathbb{F}_{q^2}$ of degree one. Then, for any $k \geq 3$, we have*

$$N_k \geq (q^2 - 1).q^{k-1} + 2q$$

COROLLARY 3.1. $\lim_{k \to \infty} N_k/g_k = q - 1$.

From this point on, let us set $M_k = (q^2 - 1).q^{k-1} + 2q$.

DEFINITION 3.1 *Let*

$$\Delta_{q,k} = M_k - (2g_k - 2) = (q^2 - 2q - 3)q^{k-1} + f(k),$$

*where*

$$f(k) = \begin{cases} 2q^{(k+1)/2} + 4q^{(k-1)/2} + 2q, & \text{if } k \equiv 1 \mod 2 \\ q^{(k/2)+1} + 3q^{k/2} + 2q^{(k/2)-1} + 2q, & \text{if } k \equiv 0 \mod 2. \end{cases}$$

*Let us consider the set*

$$\Theta_{q,k} = \{n \in \mathbb{N} \mid \Delta_{q,k} > 2n\},$$

*which, if $q \geq 3$, is not empty. Then we define the upper ray of $F_k/\mathbb{F}_{q^2}$,*

$$R_{q,k} = \sup \Theta_{q,k} = \operatorname{card} \Theta_{q,k} - 1 = \begin{cases} \lfloor \frac{\Delta_{q,k}}{2} \rfloor & \text{if } \Delta_{q,k} \text{ is odd} \\ \frac{\Delta_{q,k}}{2} - 1 & \text{if } \Delta_{q,k} \text{ is even.} \end{cases}$$

*Let us consider the set*

$$\Phi_{q,k} = \{n \in \mathbb{N} | 2g_k + 1 \leq q^{n-1}(q-1)\}$$

*which is clearly not empty. Then we define the lower ray of* $F_k/\mathbb{F}_{q^2}$,

$$\Gamma_{q,k} = \inf \Phi_{q,k}$$

*and the action domain of* $F_k/\mathbb{F}_{q^2}$

$$I_{q,k} = \Theta_{q,k} \cap \Phi_{q,k} = [\Gamma_{q,k}, R_{q,k}].$$

First, we consider the case $q > 2$.

LEMMA 3.1. *Let $q$ be a prime power $\geq 3$. Then $(\Delta_{q,k})_{k \geq 3}$ is an increasing sequence such that* $\lim_{k \to \infty} \Delta_{q,k} = \infty$.

*Proof.* Let $q$ be an arbitary prime power. For any $k \geq 3$, $\Delta_{q,k} = (q^2 - 2q - 3)q^{k-1} + f(k)$, where $f(k)$ is a positive and increasing function. Consequently, if $q > 2$, $(\Delta_{q,k})_{k \geq 3}$ is increasing and tends to infinity. ■

LEMMA 3.2. *Let $q$ be a prime power $\geq 3$. Then for any $k \geq 3$, the action domain of* $\Theta_{q,k}$,

$$I_{q,k} = \Theta_{q,k} \cap \Phi_{q,k} = [\Gamma_{q,k}, R_{q,k}],$$

*is not empty.*

*Proof.* It follows from $\Gamma_{q,k} < R_{q,k}$ for any $k \geq 3$ and for any $q \geq 3$. Indeed, it is clear that $g_k$ satisfies $2g_k + 1 \leq 2q^{k-1}(q+1)$. Moreover, for any $q \geq 3$, if $n \geq k+2$, then we have $2q^{k-1}(q+1) \leq q^{n-1}(q-1)$. Thus $\Gamma_{q,k} \leq k+2$. Further, for any $q \geq 3$, we know that $\Delta_{q,k} \geq f(k)$, which yields $R_{q,k} \geq \frac{f(k)}{2}$. Consequently, because for any $k \geq 3$ we have $k + 2 < \frac{f(k)}{2}$, we obtain $R_{q,k} > \Gamma_{q,k}$ and the proof is complete. ■

LEMMA 3.3. *Let $q$ be a prime power $\geq 3$. Then for any $k \geq 3$, $I_{q,k} \cap I_{q,k+1}$ is not empty.*

*Proof.* If follows from $\Gamma_{q,k+1} < R_{q,k}$ for any $k \geq 3$ and for any $q \geq 3$. Indeed, in the proof of Lemma 3.2, for any $k \geq 3$ and for any $q \geq 3$ we obtained $\Gamma_{q,k} \leq k+2$. Thus we have $\Gamma_{q,k+1} \leq k+3$. Moreover, $R_{q,k} \geq \frac{f(k)}{2}$. Consequently, because for any $k \geq 3$ we have $k + 3 < \frac{f(k)}{2}$, we obtain $R_{q,k} > \Gamma_{q,k+1}$ and the proof is complete. ■

LEMMA 3.4. *Let* $J_{q,\infty} = \bigcup_{k=3}^{\infty} I_{q,k}$, *then* $J_{q,\infty}$ *is a covering of* $[\Gamma_{q,3}, \infty[ \subset \mathbb{N}$.

*Proof.* First, $\Gamma_{q,k}$ is an increasing function for any $k \geq 3$. Consequently, the result immediatly follows from Lemma 3.2 and Lemma 3.3. ■

PROPOSITION 3.1. *Let* $q$ *be a prime power* $\geq 3$. *Then for any* $n > \Gamma_{q,3}$, *there exists an algebraic function field of genus* $g_k$ *having more than* $2n + 2g_k - 2$ *places of degree one and at least a place of degree* $n$. *In particular, it is true for* $n$ *such that* $n > \frac{1}{2}q^2 + 1$.

*Proof.* By [12, Corollary v.2.10.c p. 179], for any $n$ such that $2g + 1 \leq q^{(n-1)}(q-1)$, there exists at least one place of degree $n$ over an algebraic function field $F/\mathbb{F}_q$ of genus $g$. Consequently, by the definition of $I_{q,k}$ and by Lemma 3.4, for any $n \in I_{q,\infty}$, there exists an algebraic function field of genus $g_k$ having more than $2n + 2g_k - 2$ places of degree one and at least a place of degree $n$. Moreover, for any $q \geq 3$, $\Gamma_{q,3} < \frac{1}{2}q^2 + 1$ and the proof is complete. ■

*Example.* Let $q = 3$. If $k = 3$, then $\Delta_{3,3} = 30$, $g_{3,3} = 22$, $\Gamma_{3,3} = 4$ and thus, for any integer $n$ such that $3 < n < 15$, there exists an algebraic function field $F/\mathbb{F}_9$ (of genus $g = 22$) having more than $2n + 2g - 2$ places of degree one and at least one place of degree $n$. If $k = 4$, then $\Delta_{3,4} = 66$, $g_{3,4} = 79$, $\Gamma_{3,4} = 5$ and thus, $4 < n < 33$. If $k = 5$, then $\Delta_{3,5} = 78$, $g_{3,5} = 280$, $\Gamma_{3,5} = 7$ and thus, $6 < n < 39$. And so on. Consequently, for any $n > 3$ there exists algebraic function fields $F/\mathbb{F}_9$ of genus $g$ having more than $2n + 2g - 2$ places of degree one and at least one place of degree $n$.

Let us consider the case $q = 2$. Then by the Drinfeld–Vladut bound, it is clear that there exists a integer $g_0 > 0$ such that for any integer $g > g_0$, $N_q(g) - (2g - 2) < 0$. Consequently, we have the following result:

PROPOSITION 3.2. *There exists an integer* $n_0$ *such that for any integer* $n > n_0$, *there does not exist an algebraic function field of genus* $g$ *over* $\mathbb{F}_4$ *having more than* $2n + 2g - 2$ *places of degree one.*

## 4. BOUNDS ON THE MULTIPLICATION COMPLEXITY

In this section, we refine results on the multiplication complexity in $\mathbb{F}_{(q^2)^n}$, $n \in \mathbb{N}$, established in [1] and give new results from the method studied in the preceding section.

First, let us refine certain results established in [1]:

THEOREM 4.1. *Let* $q$ *be a prime power such that* $q \geq 3$ *and let* $g$ *be the genus of a maximal function field. Then for any integer* $n$ *satisfying*

$\frac{1}{2}q^2 + 1 < n < \frac{q^2+3}{2} + g(q-1)$, *we have*

$$2n \leq \mu_{q^2}(n) \leq 2n + g - 1.$$

*Proof.* By definition, an algebraic function field of genus $g$ is maximal if it is defined over $F_{q^2}$ and its number of places of degree one reaches the Hasse–Weil bound. Moreover, by a recent result due to R. Fuhrmann and F. Torres in [6], we know that its genus $g$ is such that $g \leq \frac{(q-1)^2}{4}$ or $g = \frac{q^2-q}{2}$. Consequently, the theorem is directly obtained by applying Corollary 2.1. ■

COROLLARY 4.1. *Let $q$ be a prime power such that $q \geq 3$ and $g = \frac{(m-1)(q-1)}{2}$, where $m$ is an integer such that $m > 1$ and $m|q+1$. Then for all integers $n$ such that $\frac{1}{2}q^2 + 1 < n < \frac{q^3+3}{2} + g(q-1)$, we have*

$$2n \leq \mu_{q^2}(n) \leq 2n + g - 1.$$

*Proof.* By [12], if $m$ divides $q+1$ then there exists a maximal function field of genus $g = \frac{(m-1)(q-1)}{2}$ over $\mathbb{F}_{q^2}$. Consequently, the result follows from Theorem 4.1. ■

This theorem provides us with an upper bound which depends on $g$ and therefore also on the intervals of the degrees $n$ of field extensions. This upper bound is clearly bounded by one given for the value $g = \frac{q^2-q}{2}$ with $m = q+1$ which corresponds to the Hermitian case. In this case, for any integer $n$ such that $\frac{1}{2}q^2 + 1 < n < \frac{q^3+3}{2} - \frac{q(q-1)}{2}$, we have $2n \leq \mu_{q^2}(n) \leq 2n + g - 1$. Moreover, by [13] there always exists a maximal function field called elliptic of genus $g = 1$. Thus, for any integer $n$ such that $\frac{1}{2}q^2 + 1 < n < \frac{1}{2}(q^2 + 2q + 1)$, we have $\mu_{q^2}(n) = 2n$ which is already known by Corollary 1 in [10].

*Remark.* Note that these results are now valid for $q = 3$ in contrast to these established in [1]. It is precisely Corollary 2.1 which enable us to obtain the existence of a prime divisor of degree $n$, with $q = 3$ and $n > \frac{1}{2}q^2 + 1$.

*Example.* Let $q = 4$, we know that there exist maximal function fields over $\mathbb{F}_{16}$ of genera 1, 2 and 6. Consequently, the elliptic case of $g = 1$ provides $\mu_{16}(n) = 2n$ for $9 < n \leq 12$, the hyperelliptic case of $g = 2$ gives $2n \leq \mu_{16}(n) \leq 2n + 1$ for $12 < n \leq 15$, and finally the Hermitian case of $g = 6$ gives $2n \leq \mu_{16}(n) \leq 2n + 5$ for $15 < n \leq 27$.

Now, let us give some new bounds obtained from the results of Section 3 and Theorem 1.1.

THEOREM 4.2. *Let $q$ be a prime power such that $q \geq 3$ and let $g_k$ be the integer such that for any $k \geq 3$,*

$$g_k = \begin{cases} q^k + q^{k-1} - q^{(k+1)/2} - 2q^{(k-1)/2} + 1, & \text{if } k \equiv 1 \bmod 2 \\ q^k + q^{k-1} - \frac{1}{2}q^{(k/2)+1} - \frac{3}{2}q^{k/2} - q^{(k/2)-1} + 1, & \text{if } k \equiv 0 \bmod 2. \end{cases}$$

*and*

$$M_k = (q^2 - 1).q^{k-1} + 2q.$$

*Then for all integers $n \in \mathbb{N}$ such that $n > \frac{1}{2}q^2 + 1$, we have*

$$2n \leq \mu_{q^2}(n) \leq 2n + g_{k_0} - 1,$$

*where $k_0$ is the integer such that $g_{k_0} = \min\{g_k | n < (M_k - 2g_k + 2)/2\}$.*

*Proof.* This follows directly from Proposition 3.1 and Corollary 2.1. ■

COROLLARY 4.2. *Let $q$ be a prime power such that $q > 3$. Then for any integer*

$$\mu_{q^2}(n) \leq 2\left(1 + \frac{q}{q-3}\right)n.$$

*Moreover, if $\frac{1}{2}q^{k-1}(q^2 - 2q - 3) \leq n < \frac{1}{2}q^{k-1}(q^2 - 2q - 3) + \frac{f(k)}{2}$, where*

$$f(k) = \begin{cases} 2q^{(k+1)/2} + 4q^{(k-1)/2} + 2q, & \text{if } k \equiv 1 \bmod 2 \\ q^{(k/2)+1} + 3q^{k/2} + 2q^{(k/2)-1} + 2q, & \text{if } k \equiv 0 \bmod 2, \end{cases}$$

*then*

$$\mu_{q^2}(n) \leq 2\left(1 + \frac{1}{q-3}\right)n.$$

*Proof.* For any integer $n$, let $k$ be the smallest such that $2n < M_k - 2g_k + 2$, then $2n \geq M_{k-1} - 2g_{k-1} + 2$. Consequently, we have $k - 1 \leq \log_q(2n) - \log_q(q^2 - 2q - 3) + 1$. Moreover, we have $\mu_{q^2}(n) \leq 2n + g_k - 1 \leq 2n + q^k + q^{k-1}$ by Theorem 4.2, then $\mu_{q^2}(n) \leq 2n + q^{\log_q(2n) - \log_q(q^2 - 2q - 3) + 1}(q + 1)$, i.e., $\mu_{q^2}(n) \leq 2(1 + (q/q - 3))n$. Further, if $\frac{1}{2}q^{k-1}(q^2 - 2q - 3) \leq n < \frac{1}{2}q^{k-1}(q^2 - 2q - 3) + \frac{f(k)}{2}$, then we have $k - 1 \leq \log_q(2n) - \log_q(q^2 - 2q - 3)$. Consequently, we obtain $\mu_{q^2}(n) \leq 2n + g_k - 1 \leq 2n + q^k + q^{k-1} \leq 2n + q^{\log_q(2n) - \log_q(q^2 - 2q - 3)}(q + 1)$, i.e., $\mu_{q^2}(n) \leq 2(1 + (1/q - 3))n$ and the proof is complete. ■

COROLLARY 4.3. *Let $q$ be an prime power such that $q > 3$. Then for any integer $n$,*

$$\mu_q(n) \leq 6\left(1 + \frac{q}{q-3}\right)n. \tag{3}$$

*For $q = 3$, $\mu_3(n) \leq 45n$.*
*For $q = 2$, $\mu_2(n) \leq 90n$.*

*Proof.* By Lemma 1.2 in [11], for all integers $n$ and $m$, we have $\mu_q(n) \leq \mu_q(mn) \leq \mu_q(m)\mu_{q^m}(n)$. Hence for $q > 3$, we put $m = 2$ and use $\mu_q(2) = 3$ for any $q$. Then the inequality (3) follows from Corollary 4.2. For $q = 3$ we put $m = 2$, then we use the inequality (3) and $\mu_3(2) = 3$. For $q = 2$ we put $m = 4$, then we use the first inequality of Corollary 4.2 and $\mu_2(4) = 9$ by [3]. ■

*Remark.*

(1) In particular, we see that for any prime power $q$ and any degree $n$ of the extension, the complexity of multiplication is linear in $n$.

(2) Asymptotically we obtain that for $q > 3$, $\mathscr{M}_{q^2} = \lim_{n\to\infty} \sup \mu_{q^2}(n)/n \leq 2(1 + (q/q-3))$ and for $q > 3$, $\mathscr{M}_q \leq 6(1 + (q/q-3))$. These asymptotic estimates are not as good as the estimates $\mathscr{M}_{q^2} \leq 2(1 + (1/q-2))$ and $\mathscr{M}_q \leq 6(1 + (1/q-2))$ of Shparlinski in [11] which also are valid for $q = 3$. But note that our result is valid for all $n$, not merely asymptotically. In our case, the difference in asymptotic performance is due to the use of a family of curves for which we can easily verify that the sequence of its genera is not sufficiently dense. Effectively, $\lim_{k\to\infty} \frac{g_k}{g_{k+1}} = 1/q$, which explains the presence of the factor $q$ in the bound, while in [11] $\lim_{k\to\infty} \frac{g_k}{g_{k+1}} = 1$.

(3) Moreover for the finite fields $\mathbb{F}_{q^2}$, our result is obtained from constructible curves in contrast to the modular curves used in [11]. Consequently, for any $q > 3$ and any $n$, we have found a family of bilinear multiplication algorithms which are interpolation algorithms on algebraic curves over $\mathbb{F}_{q^2}$, with a complexity linear with respect to the degree $n$ of the extension.

(4) Garcia and Stichtenoth's curves are not the only explicit curves which attain the Drinfeld–Vladut bound. Recently, Noam Elkies in [5] has shown that these curves are modular and has also obtained other sequences of function fields attaining the Drinfeld–Vladut bound. One interesting aspect of these curves is that the corresponding towers of function fields are only tamely ramified. Hence, it is conceivable that these function fields lead to a better estimate in Corollary 4.2 and Corollary 4.3. However, this is not straightforward because certain parameters of each step of the tower have to be determined.

## ACKNOWLEDGMENT

The author expresses his gratitude to R. Rolland for his supervision and to S. Vladut and H. Stichtenoth for many valuable discussions.

## REFERENCES

1. S. Ballet, On the complexity of multiplication in certain finite extensions of finite fields, Institut de Mathématiques de Luminy, Preprint 97-17, 1997.
2. P. Bürgisser, M. Clausen, and M. A. Shokrollahi, "Algebraic Complexity Theory," Grundlhehren der Mathematischen Wissenschaften, Vol. 315, Springer-Verlag, Berlin, 1997.
3. D. V. Chudnovsky and G. V. Chudnovsky, Algebraic complexities and algebraic curves over finite fields, *J. Complexity* **4** (1988), 285–316.
4. M. Deuring, "Lectures on the Theory of Algebraic Functions of One Variable," Lecture Notes in Mathematics, Vol. 314, Springer-Verlag, Heidelberg/New York/Tokyo, 1973.
5. N. Elkies, Explicit modular tower, *in* "Proceedings of the 35th Annual Allerton Conference on Communication, Control, and Computing," pp. 23–32, 1997.
6. R. Fuhrmann and F. Torres, The genus of curves over finite fields with many rational points, *Manuscripta Math.* **89** (1996), 103–106.
7. A. Garcia and H. Stichtenoth, A tower of Artin–Schreier extensions of function fields attaining the Drinfeld–Vladut bound, *Invent. Math.* **121** (1995), 211–222.
8. H. F. Groote, "Characterization of Division Algebras of Minimal Rank and the Structure of Their Algorithm Varieties," Lecture Notes in Computer Science, Vol. 245, Springer-Verlag, New York/Berlin/Heidelberg/Tokyo, 1985.
9. A. Lempel, G. Seroussi, and S. Winograd, On the complexity of multiplication in finite fields, *Theoret. Comput. Sci.* **22** (1983), 285–296.
10. M. A. Shokrollahi, Optimal algorithms for multiplication in certain finite fields using algebraic curves, *SIAM J. Comput.* **21**, No. 6 (1992), 1193–1198.
11. I. E. Shparlinski, M. A. Tsfasman, S. G. Vladut, "Curves with Many Points and Multiplication in Finite Fields," Lecture Notes in Mathematics, Vol. 1518, pp. 145–169, Springer-Verlag, Berlin, 1992.
12. H. Stichtenoth, "Algebraic Function Fields and Codes," Lecture Notes in Mathematics, Vol. 314, Springer-Verlag, Berlin/Heidelberg/New York, 1993.
13. W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Sci. Ecolo. Norm. Sup.* **4** (1969), 521–560.
14. S. Winograd, On multiplication in algebraic extension fields, *Theoret. Comput. Sci.* **8** (1979), 359–377.